PONDURANCE

2020 CYBER
INSURANCE & THREATS

4 Lessons Learned

pondurance.com

If anything, 2020 has been about preparing for *everything*. This includes cyberthreats, which have risen sharply in the pandemic era.[1] Nearly 4 out of 5 organizations have acquired cyber insurance coverage (up from 34% in 2011)[2] to protect themselves from these threats. Here are four lessons learned about threats and cyber insurance in 2020 to help your organization make informed, cost-effective decisions moving forward.

Nearly **4 OUT OF 5** organizations have acquired cyber insurance coverage to protect themselves from threats.[2]

The FBI cites

$3.5 billion

in cybercrime losses
reported in 2019

PONDURANCE

Unavoidable Outcome of Widespread Cyber Insurance Coverages

It's unavoidable, as more organizations add cyber insurance coverage, that cybercriminals are going to be interested and looking for ways to take advantage. Cybercriminals may assume that if a company they attack is insured, the claim *will* get paid. Investigators are even seeing scenarios where criminals are compromising companies, obtaining their insurance coverage information as part of their surveying, and then aligning their ransomware terms to the policy details so their demands result in the victim organizations being reimbursed. In doing so, criminals reason this increases the probability of payment since the victim knows the insurer will ultimately pay for the ransom.

It is up to the client, not the carrier, to ultimately decide if they will pay the ransom. Brian Thornton, CEO of ProWriters, shared that his company has "seen a recent reduction in ransom payments — possibly due to companies having better segmentation and backups and not needing to pay the ransom to restore operations." He added that "as more cybercriminals are being added to the OFAC list, that would not allow a company or insurer to pay a ransom."

The goal is to protect all data in your environment, but it is important to put extra emphasis on protecting your cyber insurance policy information.

Learn more about ransomware attacks in our whitepaper:
Stop the Spread of Ransomware

Beating Ransomware to the "Tipping Point" Helps Keep Risk (and Ideally Premiums) Manageable

99%
of large-scale
RANSOMWARE EVENTS
spread through domain controllers

Of course, organizations have layered security controls, but cyber insurance equations focus on what happens when these are inevitably defeated or bypassed. How would you spot an intrusion and regain the upper hand against laterally moving malware stealing, wiping, or ransoming files? The alternative is an attacker making it to the crown jewels of the most sensitive data and software that handle the most sensitive crossroads of access control, credentials, and system administration. When the latter are compromised, incidents can rapidly cascade out of control, putting victims in the uncomfortable position of having to contemplate paying ransoms or moving forward without irreplaceable data.

No two organizations are the same, but experience shows that domain controllers are the crucial high ground to defend and hold.[3] Your domain controller acts as the enterprise gatekeeper for security authentication requests to allow network and user account access. In our research, we've found that **99% of large-scale ransomware events spread through domain controllers**. Given this, it clearly makes good business sense to invest in the continuous monitoring, penetration testing, and vulnerability scanning of the domain controller environment to thwart these attacks. Such initiatives can lessen the impact of ransomware incidents, reducing risk and improving overall cybersecurity posture.

Learn more about domain controller compromises and the best ways to protect your environment in our whitepaper: The Domain Controller...An Achilles Heel

It's Critical To Know Exactly What's Covered

In two high-profile lawsuits contesting denial of coverage over the 2017 NotPetya attacks, pharmaceutical giant Merck is seeking $1.3 billion from multiple insurers, and multinational food company Mondelez International claims it is owed $100 million from its providers. In both disputes, the insurance providers cite war and terrorism exclusions[4] to deny the claims under their property policies. Brian emphasizes knowing exactly what is covered and what is not under a policy. He states that "should a company like this have a stand-alone cyber tower, this type of event should be able to be covered, which also places an importance on the brokers and carriers that you work with."

Fortunately, we're seeing insurers more often opting to pay out instead of denying claims. But there are plenty of gray areas. For example, if a state actor launches a hack or if an incident *appears* that way, does that purported linkage constitute an act of war?

Enterprise security and risk leaders must completely understand where threats are likely to come from and make sure the ensuing potential losses are included in policies. Thoroughly understanding cybersecurity coverage and having policies to cover different scenarios are critical to ensure exclusions don't preclude an event from being covered.

Learn more about insurance coverage in our whitepaper:
Why DFIR Is Needed in Partnership With Cyber Insurance

$18 billion
in losses
FROM 100 LARGEST
cyber incidents in last 5 years
(Cyentia[5])

PONDURANCE

Enlisting a Cybersecurity Partner is an Overlooked Step

HAVING A CYBERSECURITY PARTNER IS CRUCIAL FOR HELPING COMPANIES BUY THE RIGHT COVERAGE AND PROVIDE THE FACT BASE FOR CLAIMS.

Partnering with cybersecurity experts that provide digital forensics and incident response (DFIR) services can help you swiftly contain incidents and conclusively restore systems after an attack. By engaging with a DFIR provider in advance of a breach, the provider's team will be familiar with your organization and have an understanding of your network in the event of a cyber incident.

There is also the option of enlisting a managed detection and response (MDR) provider to reduce the likelihood of a breach. Advanced MDR providers monitor networks 24/7, find suspicious activity, and launch effective mitigation measures if an incident occurs. This decreases dwell time, the number of days, weeks, or even months that a threat can hide within a network and compromise data.

2020 Saw a

56-day

MEDIAN DWELL TIME

(M-Trends[6])

With both types of cybersecurity partnerships in place, companies can both reduce incidents and demonstrate to insurance providers that they are taking responsible steps to pursue comprehensive defense strategies. In turn, these companies greatly lower their risk profiles, which can ultimately help in reducing premiums. If a compromise occurs, the insurance provider will be more likely to cover the incident based on the necessary precautions that the company has taken. Additionally, the cybersecurity partner will serve as a trusted representative, working with the insurance provider to accelerate the recovery process. This leads to far better results than starting from scratch in the heat of a breach, which is critical.

The only certainty about cyberthreats is uncertainty. As cyberattacks continue to evolve, cyber insurance makes changes to keep up. It is important to know what is covered in your policy to ensure it covers all your potential risks.

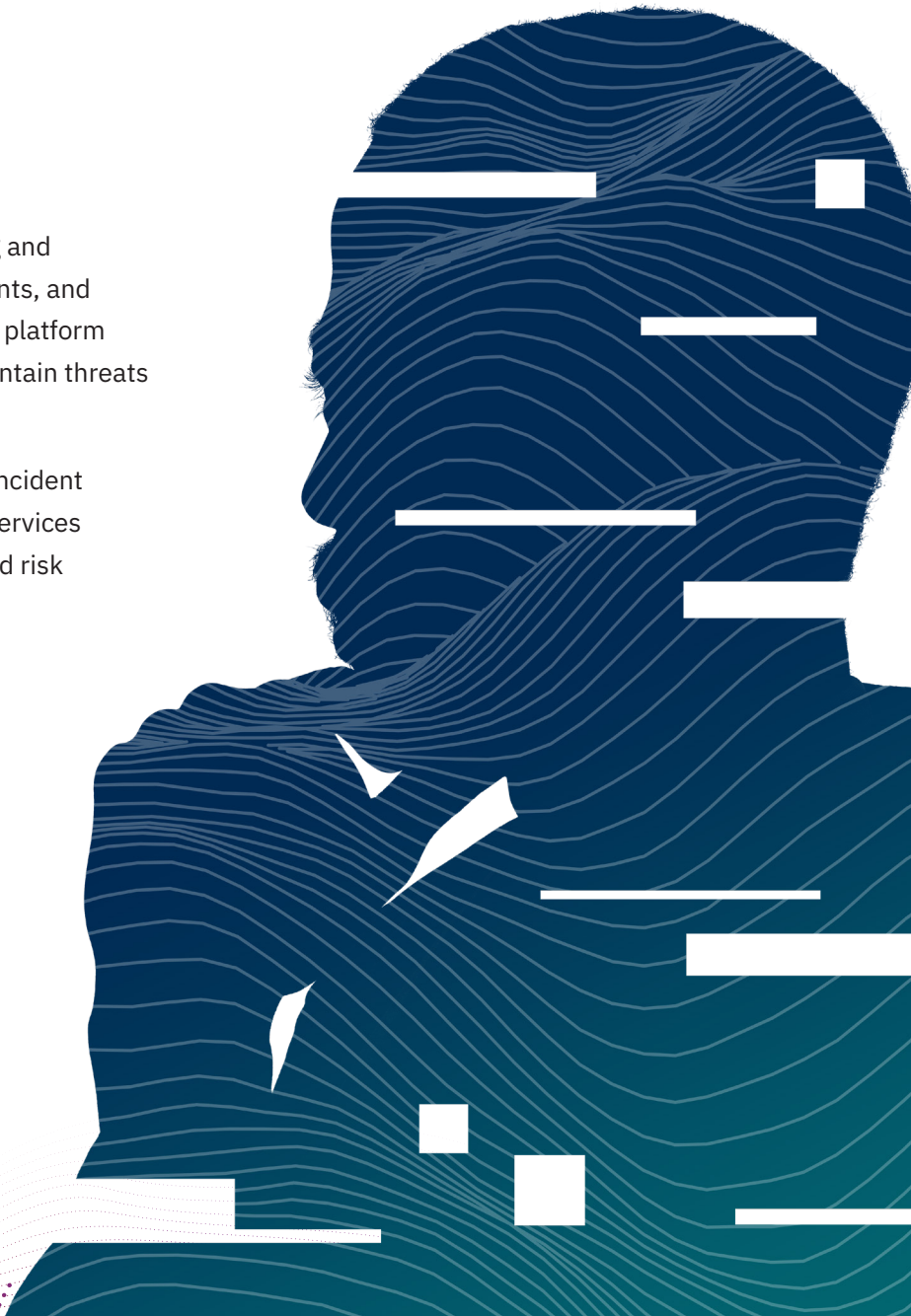
PONDURANCE

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



Sources:
1. Voice of America, UN Warns Cybercrime on Rise During Pandemic, May 2020.
2. Advisen, 10th Annual Information Security and Cyber Risk Management Survey, 2020.
3. NIST, Computer Security Resource Center.
4. Insurance Business America, Why war exclusions need to evolve for cyber insurance to be effective, Dec 2020.
5. Cyentia Institute, IRIS 20/20 Information Risk Insights Study Xtreme, 2020.
6. FireEye, M-Trends 2020: Insights From the Front Lines, Feb 2020.

pondurance.com

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204